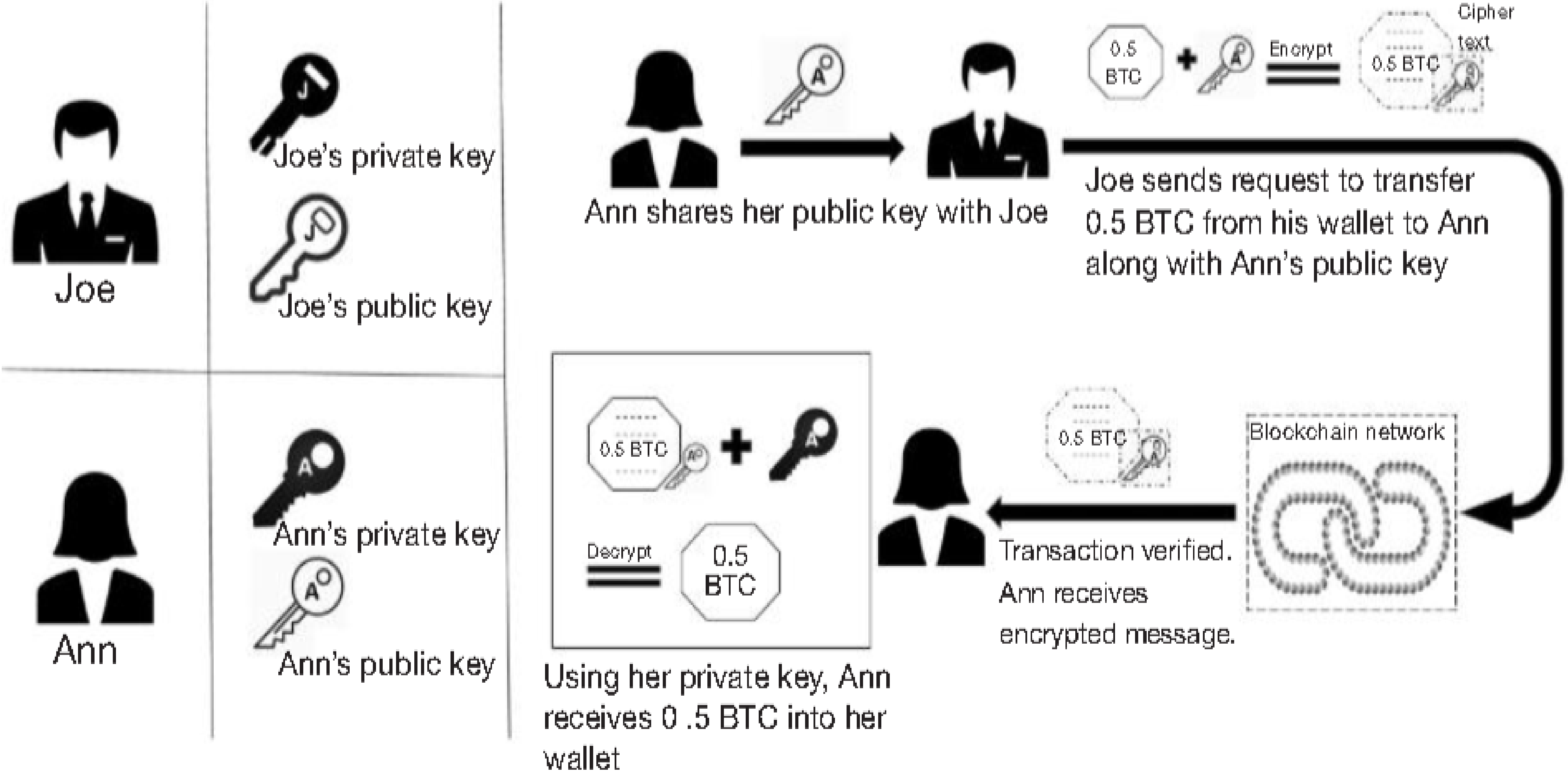
Public-key cryptography, or asymmetric cryptography, is a cryptographic system which uses pairs of keys: public keys, and private keys. The generation of such key pairs depends on cryptographic algorithms which are based on mathematical problems termed one-way functions.

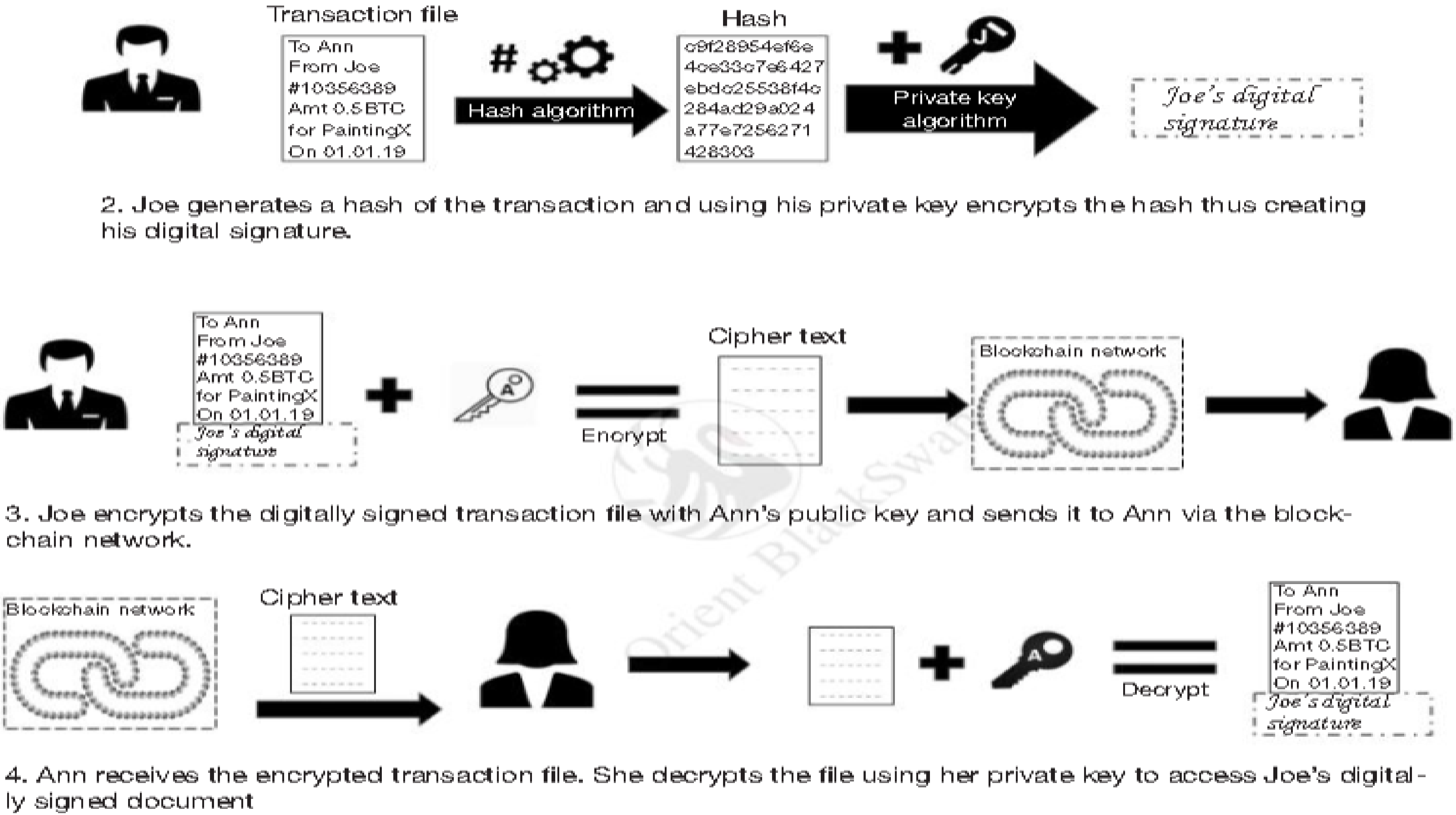


Ann shares her public key with Joe

Joe sends request to transfer 0.5 BTC from his wallet to Ann along with Ann's public key

Transaction verified. Ann receives encrypted message.

Using her private key, Ann receives 0 .5 BTC into her wallet

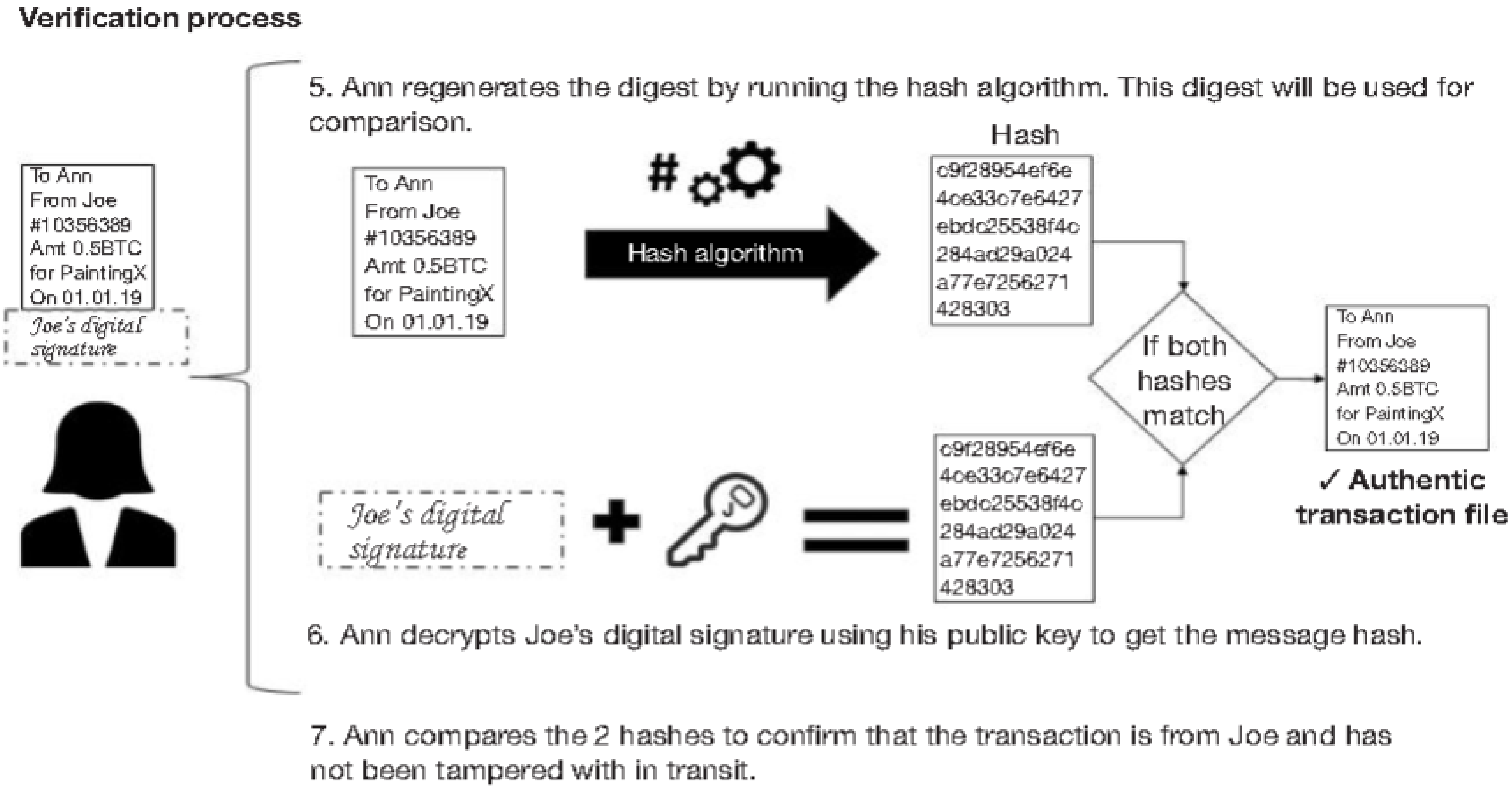


2. Joe generates a hash of the transaction and using his private key encrypts the hash thus creating his digital signature.

3. Joe encrypts the digitally signed transaction file with Ann's public key and sends it to Ann via the blockchain network.

4. Ann receives the encrypted transaction file. She decrypts the file using her private key to access Joe's digitally signed document

Figure 1.6: Digital signature



Verification process

5. Ann regenerates the digest by running the hash algorithm. This digest will be used for comparison.

6. Ann decrypts Joe's digital signature using his public key to get the message hash.

7. Ann compares the 2 hashes to confirm that the transaction is from Joe and has not been tampered with in transit.

Figure 1.7: Verification

Table 1.2 Step-by-step representation of a blockchain transaction

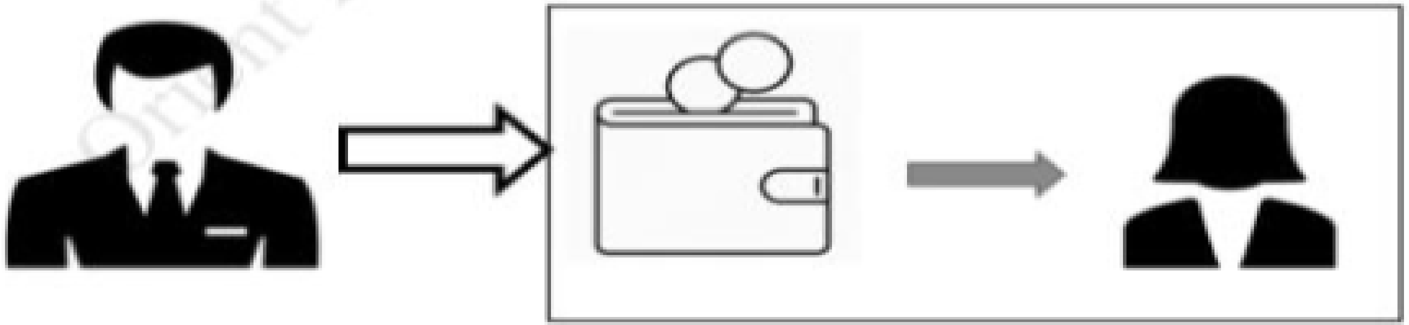
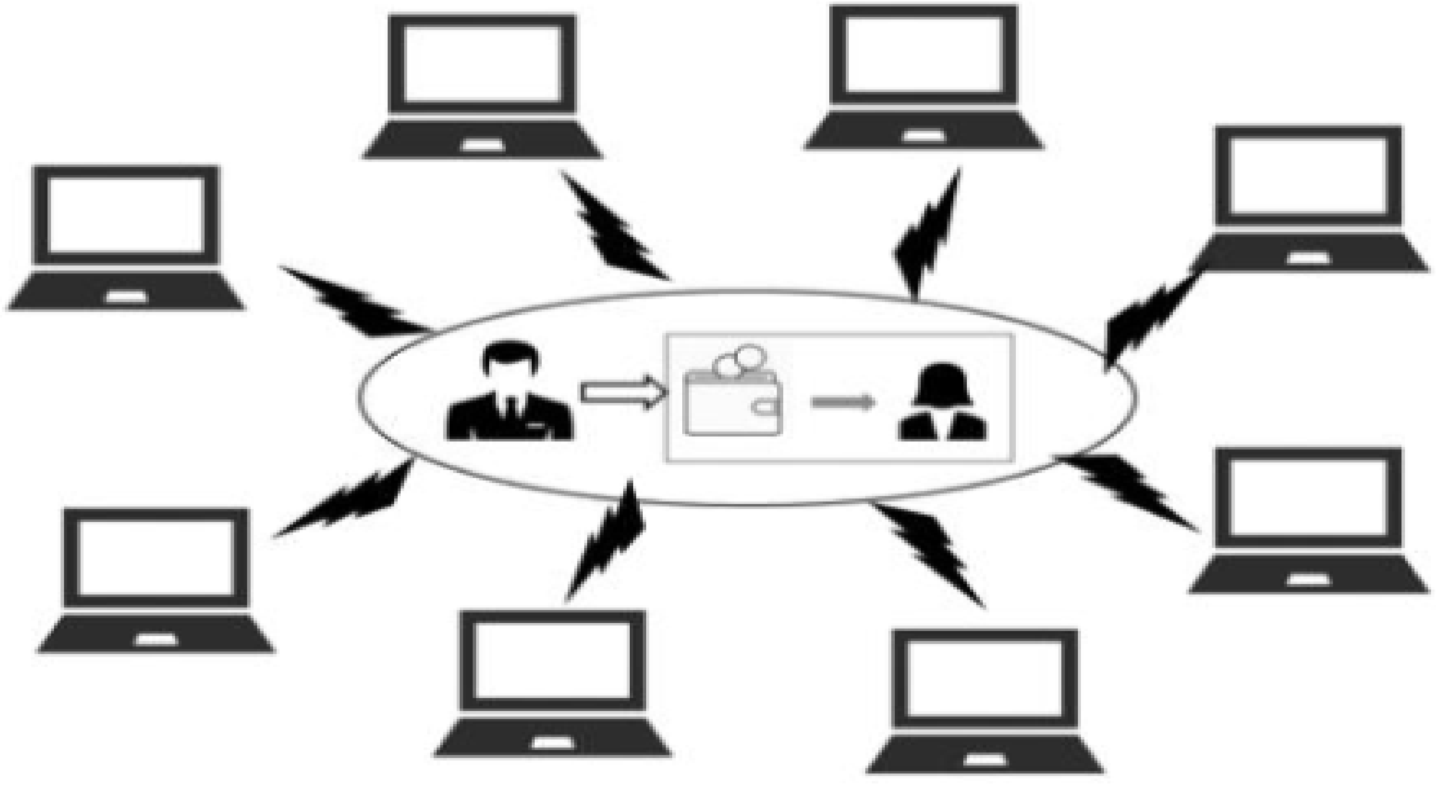
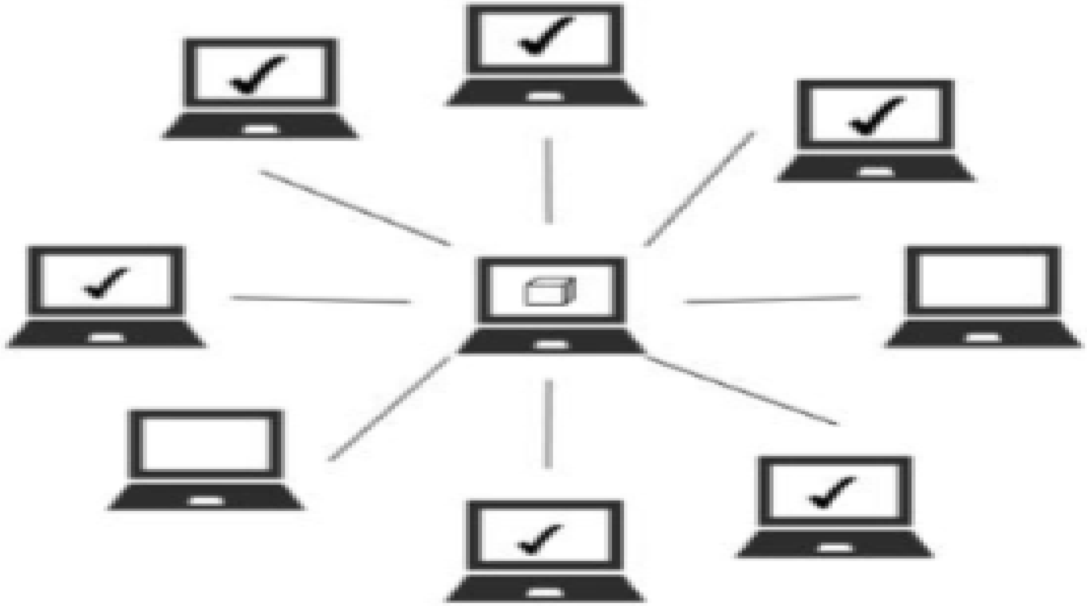
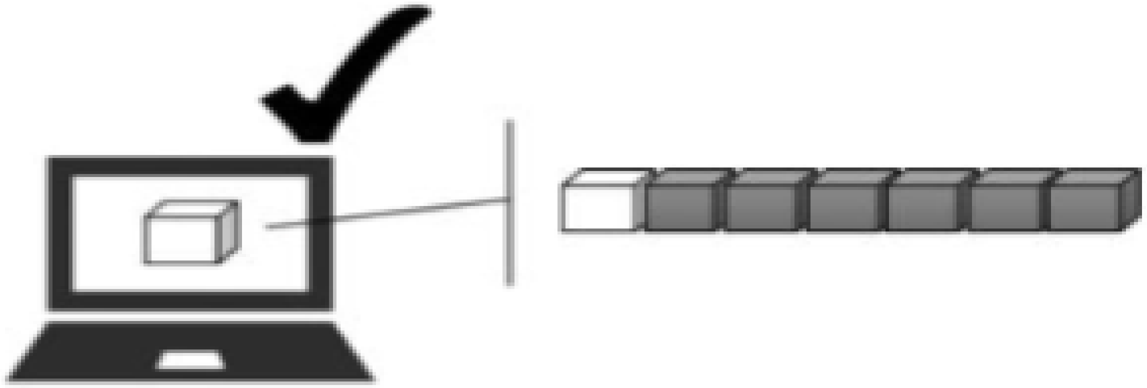
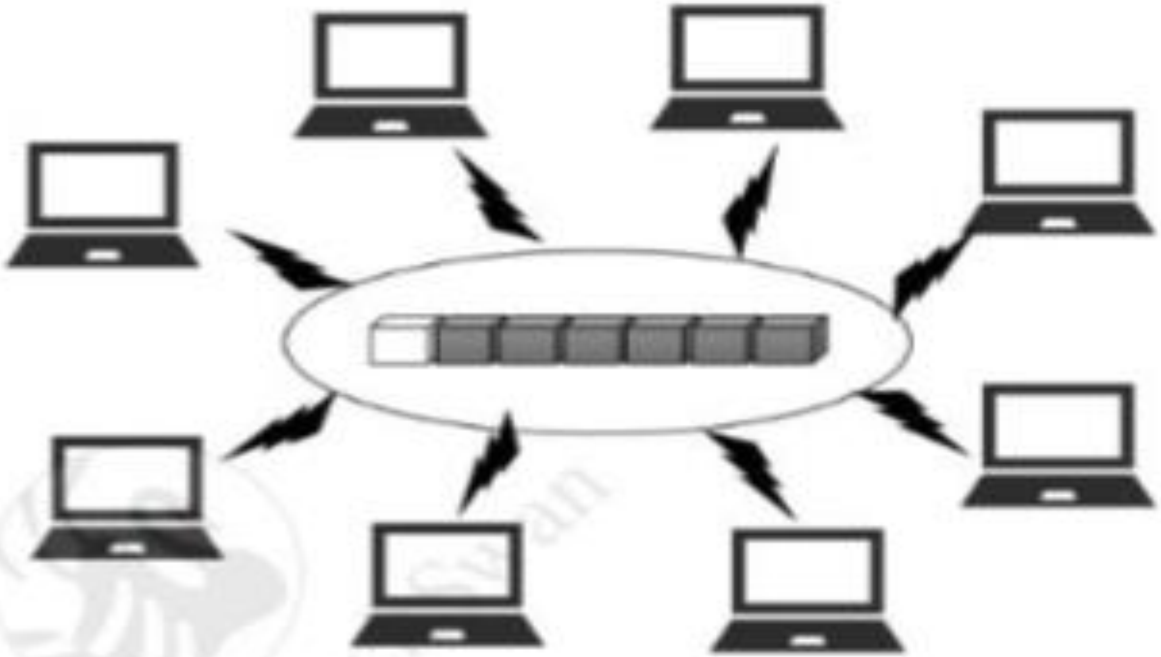
Step 1: Joe requests the proposed transaction Joe sends 0.5 BTC from his Wallet app.	
Step 2: The proposed transaction is broadcast to the network	

Table 1.2 *(Continued)*

Step 3: Miners verify the transaction and bundle it into a block along with other transactions. – The miner will validate the authenticity of the transaction, i.e., the status of Joe, his balance, etc. **Note**: Miners validate all the transactions they wish to include in the block they plan to mine.	
Step 4: Miners compete to solve the complex mathematical puzzle. – The puzzle requires much computational power to solve. – This protects the blockchain against hackers as it would be difficult and expensive to attack the network.	

Step 5: The nodes verify the miner's work. – The miner who finds the correct hash broadcasts the block to the network – Majority of the nodes/miners need to approve/verify the block for it to be accepted into the blockchain – Once approved, the winning miner can collect his reward.	
Step 6: Block is added to the blockchain. – Once the block is verified, the winning miner adds his block to the existing blockchain. **Note**: Joe's transaction is added to the blockchain along with the other transactions	

Step 7: The updated copy of the blockchain is circulated throughout the network.	
Step 8: Transaction completion Ann receives 0.5 BTC in her wallet. The transaction is complete.